Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC

Hearing on

H.R. 98,
the "Illegal Immigration Enforcement and
Social Security Protection Act of 2005"

Before the

Subcommittee on Immigration, Border Security, and Claims,
Committee on the Judiciary,
U.S. House of Representatives

May 12, 2005
2141 Rayburn House Office Building
Washington, DC

Introduction

Chairman Hostettler, Ranking Member Jackson Lee, and Members of the Subcommittee, thank you for the opportunity to testify on H.R. 98, the "Illegal Immigration Enforcement and Social Security Protection Act of 2005." My name is Marc Rotenberg and I am Executive Director of the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C. Founded in 1994, EPIC has participated in cases involving the privacy of the Social Security Number (SSN) before federal courts and has frequently testified in Congress about the need to establish privacy safeguards for the Social Security Number.[1] EPIC maintains an archive of information about the SSN online at http://www.epic.org/privacy/ssn/.

Today, I will provide an analysis of H.R. 98, the "Illegal Immigration Enforcement and Social Security Protection Act of 2005," from a privacy and civil liberty rights perspective. The bill would significantly increase the use of the Social Security Number. Further, the bill would transfer SSN record information from the Social Security Administration to the Department of Homeland Security, and would dramatically expand the mission of DHS to include determining who is eligible to work in the U.S. Finally, the bill does not include adequate privacy and security safeguards.

I. H.R. 98 Would Turn the SSN Into a National Identifier and Increase the Risk of Identity Theft

The United States Congress has a long-standing concern about the misuse of the Social Security Number. In passing the Privacy Act of 1974, Congress specifically limited the use of the SSN and rejected the establishment of a federal data center for personal information. A 1977 report issued as a result of the Privacy Act highlighted the

[1] See, e.g., Greidinger v. Davis, 988 F.2d 1344 (4th Cir. 1993) ("Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling"); Beacon Journal v. Akron, 70 Ohio St. 3d 605 (Ohio 1994) ("the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs"); Testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, at a Joint Hearing on Social Security Numbers and Identity Theft, Joint Hearing Before the House Financial Services Subcommittee on Oversight and Investigations and the House Ways and Means Subcommittee on Social Security (Nov. 8, 2001) *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Testimony of Chris Jay Hoofnagle, Legislative Counsel, EPIC, at a Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the House Ways and Means Subcommittee on Social Security and the House Judiciary Subcommittee on Immigration, Border Security, and Claims (Sept. 19, 2002) *available at* http://www.epic.org/privacy/ssn/ssntestimony9.19.02.html.

dangers and transfers of power from individuals to the government that occur with centralization of personal information:

> In a larger context, Americans must also be concerned about the long-term effect record-keeping practices can have not only on relationships between individuals and organizations, but also on the balance of power between government and the rest of society. Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly. Thus, growth in society's record-keeping capability poses the risk that existing power balances will be upset.[2]

Creation of a nationwide system of SSN verification across public agencies and private businesses will upset balances of power described in the 1977 report and reduce individuals' autonomy from both government and commercial entities. The creation of a national ID runs counter to public sentiment and recent congressional action.[3]

This concern is not new; it was voiced at the creation of the SSN and has since been raised repeatedly. The SSN was created in 1936 for the sole purpose of accurately recording individual worker's contributions to the social security fund. The public and legislators were immediately suspicious and distrustful of this tracking system fearing that the SSN would quickly become a system containing vast amounts of personal information, such as race, religion and family history that could be used by the government to track down and control the action of citizens. Public concern over the potential for abuse inherent in the SSN tracking system was so high, that in an effort to dispel public concern the first regulation issued by the Social Security Board declared that the SSN was for the exclusive use of the Social Security system.

The use of the SSN as the means of tracking every employment encounter will expand the amount of information accessible to the unscrupulous individual who has obtained another's SSN. The development of a machine-readable SSN will facilitate linkage between various systems of governmental and private sector records further eroding individual privacy and heightening surveillance of each American's life.

Supporters of H.R. 98 have tried to address public concerns about the creation of a national identification card by including a disclaimer in the bill stating: "This card shall not be used for the purpose of identification."[4] However, the bill would create a national ID card in practice.

---

[2] Privacy Prot. Study Comm'n, Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission (1977), *available at* http://www.epic.org/privacy/ppsc1977report/c1.htm.

[3] For instance, the Department of Homeland Security is expressly prohibited from developing National ID systems. 6 USCS § 554 (2004).

[4] Illegal Immigration Enforcement and Social Security Protection Act, H.R. 98, 109th Cong., §3(a)(3) (2005).

The bill, should it become law, would require each citizen and non-citizen in the U.S. to provide this new national identify card to each prospective employer. It also requires Homeland Security to create a database containing information on employment eligibility, as well as information on all citizens and non-citizens living in the country legally. Section 9, the Integration of Fingerprinting Databases, directs the Secretary of Homeland Security and the Attorney General of the United States to integrate fingerprint databases maintained by the both agencies. The two databases were created for specific purposes. But essential privacy safeguards have been removed. In 2003 the Justice Department's decision to lift the Privacy Act requirement that the FBI ensure the accuracy and completeness of the over 39 million criminal records it maintains in its National Crime Information Center (NCIC) database. This action continues to pose significant risks to both privacy and effective law enforcement.

The bill proposes that this new identification card would be swiped through an electronic card reader or the employer would contact the Department of Homeland Security to verify that the number is present in their database in an attempt to verify the job applicant's identity. Employers, facing stiff penalties for hiring ineligible workers, likely would use the SSN card as a de facto identification card, no matter what disclaimer was placed onto the card.

H.R. 98 also expands use of the new SSN card in another way. Under the "Confidentiality" provision of the bill, it restricts the use of the proposed DHS employment eligibility database to those required for the administration of H.R. 98 or for "any other purpose the Secretary of Homeland Security deems to be in the national security interests of the United States."[5] This "any other purpose" clause in H.R. 98 raises the risk of mission creep. It is unknown what these other purposes may be, but they will likely not be related to employment eligibility, which is the stated reason for the establishment of the database.

The Department of Homeland Security has already shown a proclivity for using personal information for reasons other than the ones for which the information was gathered. Documents about the CAPPS II program collected by EPIC under the FOIA clearly showed that the Transportation Security Administration had considered using personal information gathered for the CAPPS II program for reasons beyond its original purposes. For example, TSA stated that CAPPS II personal data might be disclosed to federal, state, local, international or foreign agencies for their investigations of statute, rule, regulation or order violations.[6]

II. The Bill Dramatically Expands the Mission of DHS to Include Employment Eligibility Verification

[5] H.R. 98 at §4(c)(1)(B).

[6] Department of Homeland Security TSA, *Draft Privacy Impact Statements (CAPPS II)*, April 17, 2003, July 29, 2003, and July 30, 2003, obtained by EPIC through FOIA litigation, *available at* http://www.epic.org/privacy/airtravel/profiling.html.

The new Department of Homeland Security (DHS) has three primary missions: Prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage from potential attacks and natural disasters. Adding to this short list of critical responsibilities to our nation and its citizens would jeopardize the core mission and impetus for the creation of this agency. Further, the role of employment verification and use of the SSN is not compatible to the make up or focus of the agency. The SSN is not just about working in our nation, but provides the means of ensuring retirement security to our nation's elderly. Changing how the SSN is administered might have unintended consequences for our nation's premier retirement security program.

H.R. 98 would shift SSN information records, and possibly the management of the database itself, from the Social Security Administration to the Department of Homeland Security. The bill would create at least 10,000 positions in Homeland Security, which already has 180,000 employees, for management of the SSN system.[7] This is a dramatic expansion of the mission of Homeland Security into the realm of employment eligibility.

Divisions in the less than three-year-old Department of Homeland Security already are suffering serious setbacks. Just a few days ago, the *New York Times* reported that DHS will spend billions to alter or replace antiterrorism equipment that it has already spent $4.5 billion on.[8] Also, the Transportation Security Administration's current aviation program to screen passengers and their luggage for threatening objects recently was found to be woefully inadequate by the Government Accountability Office. The GAO found that there has been only modest progress in how well screeners detect threat objects following a report last year that documented gaps in screener security.[9] The Department of Homeland Security has significant responsibilities. Taking management of the SSN away from the SSA, which has been administering the system since its creation 70 years ago, and placing employment eligibility verification and employer sanctions into the hands of Homeland Security seems inefficient at best.

III. H.R. 98 Does Not Include Adequate Privacy and Security Safeguards

Privacy and security interests are protected best by identity documents that serve limited purposes and by reliance upon multiple and decentralized systems of identification in cases where there is a genuine need to establish identity. Centralizing authority over personal identity necessarily increases both the risk of identity theft as well as the scope of harm when identity theft occurs.

---

[7] *Id.* at §8.

[8] Eric Lipton, *U.S. to Spend Billions More to Alter Security Systems*, New York Times, May 8, 2005.

[9] Government Accountability Office, *Transportation Security: Systematic Planning Needed to Optimize Resources, Statement of Cathleen A. Berrick, Director Homeland Security and Justice*, GAO-05-357T (Feb. 15, 2005) ("GAO Report")

An employment eligibility database containing SSNs and other personal information would provide too attractive a target to identity thieves seeking to create false identities for criminal endeavors. The Government Accountability Office has stated in congressional testimony concerning the need to protect the integrity of the SSN that:

> [t]o the extent that personal information is aggregated in public and private sector databases, it becomes vulnerable to misuse. In addition, to the extent that public record information becomes more available in an electronic format, it becomes more vulnerable to misuse. In addition, to the extent that public record information becomes more available in an electronic format, it becomes more vulnerable to misuse.[10]

H.R. 98 does not once mention "privacy." The bill has two references to "safeguard."[11] There is vague language discussing protection of the SSN and other sensitive personal information in the employment eligibility database under the "Confidentiality" subsection.[12] The bill states that database access will be restricted to those employees whose "duties or responsibilities require access for the purposes described in paragraph (1)." Paragraph (1) restricts the use of the proposed DHS employment eligibility database to those required for the administration of H.R. 98 or for "any other purpose the Secretary of Homeland Security deems to be in the national security interests of the United States."[13] It is conceivable that many employees whose responsibilities do not remotely connect with employment eligibility verification will have access to the database.

Security is vital with any computerized system, which also includes those containing personally identifiable information such as the one proposed by H.R. 98. In any computer system, whether centralized or distributed, there are security threats. There are also threats to a decentralized computer systems, called distributed networks, which require periodic connection to a centralized system. Computer security should be approached as an end-to-end task that must include all parts of the system's hardware, software, computer disks, tapes, personnel, etc.

H.R. 98 does not afford the sensitive information in the database any specific safeguard beyond the above access restriction. The bill states that the "Secretary [of Homeland Security] shall provide such other safeguards as the Secretary determines to be necessary or appropriate to protect the confidentiality of information contained in the Database."[14] The Department of Homeland Security has a history of exempting many of

---

[10] General Accounting Office, *Social Security Numbers: Ensuring the Integrity of the SSN, Statement of Barbara D. Bovbjerg, Director, Education, Workforce, and Income Security Issues*, GAO-03-941T at 12 (July 10, 2003).
[11] H.R. 98 at §4(c).
[12] *Id.* at §4(c)(3).
[13] *Id.* at §4(c)(1)(B).
[14] *Id*. at §4(c)(1)(C).

its programs from the provisions of the Privacy Act of 1974. and not conducting required Privacy Impact Assessments.[15] In this climate of heightened awareness of identity theft, it is essential that such sensitive information have strong, specific safeguards against misuse or abuse.

At the very least, the Subcommittee should prohibit the use of this card for any purpose other than determining employment eligibility, and should impose significant civil penalties for violations.

IV. Conclusion and Ongoing Concerns about REAL ID

Mr. Chairman, Members of the Subcommittee, this week the Senate passed the supplemental appropriations for the troops in Iraq and for tsunami relief. The bill also included the REAL ID Act. This was a controversial measure and a controversial manner to pass legislation. I will not go into all of the debate about the REAL ID Act, but it is appropriate at this hearing on the SSN to explain why it is important to fully assess the risks of new systems of identification.

In passing the REAL ID Act, the Congress mandated the collection of sensitive personal information by the state DMVs at the same time that the state DMV record systems have become the target of identity thieves. In recent months, identity thieves have attacked three state DMVs. In March, burglars rammed a vehicle through a back wall at a DMV near Las Vegas and drove off with files, including Social Security numbers, on about 9,000 people. Recently, Florida police arrested 52 people, including 3 DMV examiners, in a scheme that sold more than 2,000 fake driver's licenses. Two weeks ago, Maryland police arrested three people, including a DMV worker, in a plot to sell about 150 fake licenses.[16] Instead of investigating this growing problem, Congress passed legislation that will require us all to give state DMVs the very documents that establish our identity.

With this legislation, H.R. 98, Congress would be mandating increased dependence on the Social Security Number at a time when we know that the SSN contributes to identity theft and undermines personal privacy. What will happen, for example, when merchants routinely ask individuals to present their SSN with the magnetic stripe to verify a credit card or check purchase? What about entry to a bar, a federal office building, or an amusement park? Has any thought been given to the

---

[15] Examples include the CAPPS-II, Registered Traveler, Secure Flight, and Transportation Worker Identity Credential programs. *See generally* EPIC's Air Travel Privacy page at http://www.epic.org/privacy/airtravel/. See, also, "Homeland Security Information Network Criticized," *The Washington Post*, May 10, 2005, at A08 ("A Department of Homeland Security network that shares classified information with intelligence and law enforcement agencies was put together too quickly to ensure it can protect the information, according to the department's acting inspector general.")

[16] See EPIC, "National ID Card and REAL ID Act" http://epic.org/privacy/id_cards/.

dramatic increase in the collection and use of the SSN that will result if this bill is passed?

It is tempting to believe that technology and new systems of identification can help solve long-running policy problems, such as determining eligibility to work in the United States. But the reality may be that new systems of identification will create new risks.

It is clear the SSN was never intended to be a national identifier, and should not be used as such. H.R. 98 has substantial weaknesses. We urge the Subcommittee to limit the use of the Social Security Number. We also urge the Subcommittee to create strong safeguards for the sensitive personal information of every American eligible to work.